Deutscher Bundestag
13. Wahlperiode

Drucksache 13/3932

13. 02. 96

Kleine Anfrage

des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Sicherheit der Informationstechnik und Kryptierung

Die Bedeutung der Sicherheit der Informationstechnik (IT-Sicherheit) wird häufig betont. Die Praxis zeigt jedoch, daß Probleme von großer Wichtigkeit nicht angegangen und grundsätzliche Fragen nicht gestellt werden. In besonderem Maße tritt dies bei solchen technischen Teilbereichen zutage, die wie die Kryptographie nicht allein der Herstellung von IT-Sicherheit dienen können, sondern den Interessen staatlicher Sicherheit untergeordnet werden.

Die Bundesregierung bereitet derzeit die Einführung einer elektronischen Unterschrift vor. Elektronische Daten werden dabei durch eine Verschlüsselung „versiegelt". Gleichzeitig wird auf diese Weise die Nutzung von kryptographischen Verfahren in großem Umfang begonnen. Pläne seitens der EU-Kommission zu ähnlichen Verfahren sind bekanntgeworden, die US-Regierung hat ihrerseits erste Überlegungen einer Neuausrichtung ihrer Kryptographie-Politik bekanntgegeben. Die Antwort der Bundesregierung auf eine Anfrage zur Kryptographie (Drucksache 13/1889) ist damit nicht länger aktuell.

Der bislang nicht gewährleistete Schutz persönlicher Daten, die auf elektronischem Weg verschickt werden, kann mit den Kryptierungsinitiativen vorangetrieben werden. Damit wird gleichzeitig die Frage nach einer internationalen Abstimmung notwendig, wenn Nutzung wie Handel mit Kryptiersystemen keinen künstlich errichteten Barrieren ausgesetzt werden sollen.

IT-Sicherheit besteht jedoch aus weit mehr als nur Kryptierung. Da nach der Antwort der Bundesregierung auf eine Kleine Anfrage zum Bundesamt für Sicherheit in der Informationstechnik (BSI) (Drucksache 13/3408) noch viele Fragen offengeblieben sind, ist es notwendig, verschiedene Bereiche der IT-Sicherheit erneut zu thematisieren.

Wir fragen die Bundesregierung:

1. Gibt es offizielle Kontakte zwischen Mitarbeitern des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Mitarbeitern der National Security Agency (NSA)?

   Wenn ja, in welchen Gremien, zu welchem Zweck, wann und aus welchem Anlaß fand die letzte Begegnung statt?

2. Welche offiziellen Kontakte gab es zwischen der NSA und Mitarbeitern der ehemaligen Zentralstelle für das Chiffrierwesen (ZfCh), und in welchem Umfang werden diese heute vom BSI weitergepflegt?

3. Mit welchen Unternehmen hat die ZfCh bei der Entwicklung von Verschlüsselungstechnik zusammengearbeitet bzw., mit welchen arbeitet das BSI heute zusammen?

4. Gab bzw. gibt es dabei eine Zusammenarbeit mit Firmen der Nachrichtentechnik sowie Herstellern von Geräten und Systemen zur Elektronischen Kampfführung (EloKa)?

   Wenn ja, mit welchen und zu welchem Zweck?

5. Trifft es zu, daß für das BSI ein neuer leistungsfähiger Großrechner beschafft werden soll?

   Wenn ja, für welche Zwecke wird dieser Rechner benötigt?

6. In welchem Umfang unterliegt der Export von Verschlüsselungssystemen in der Bundesrepublik Deutschland Exportbeschränkungen, und in welchem Umfang ist das BSI an der Erteilung von Exportlizenzen fachlich beteiligt bzw. war die vormalige ZfCh daran beteiligt?

7. Beabsichtigt die Bundesregierung regulative Änderungen bei der Vergabe von Exportlizenzen?

8. Ist der Bundesregierung eine Einflußnahme von für Kryptierungsfragen zuständigen Behörden auf die Entwicklung von Kryptiersystemen bekannt?

9. Ist der Bundesregierung eine Einflußnahme von für Kryptierungsfragen zuständigen Behörden auf die Exportfähigkeit von Kryptiersystemen bekannt?

10. Ist der Bundesregierung die Ansicht von Kryptierexperten bekannt, bestimmte Verschlüsselungsstandards und -systeme seien durch Einflußnahme von für Kryptierungsfragen zuständigen Behörden, insbesondere der NSA, aufgeweicht worden, und welche Konsequenzen zieht sie hieraus?

11. Ist der Bundesregierung bekannt, aus welchem Grund die International Standards Organization (ISO) ihren Gliederungen – Technical Committees – die Normung von Kryptieralgorithmen verboten hat?

    Wenn ja, welche Position hat die Bundesregierung dabei vertreten?

12. Welche Folgerungen zieht die Bundesregierung aus Berichten (Computer Zeitung vom 25. Januar 1996), daß der Soft-

warehersteller Lotus zur Erlangung einer Exportlizenz in den USA für die neue Version 4.0 seines Produktes Lotus Notes 24 der 64 Bits des Kryptierschlüssels US-Behörden bekanntgeben mußte?

13. Ist diese Software bei Bundesbehörden im Einsatz?

    Wenn ja, bei welchen?

14. Hat die Bundesregierung bei der Beratung der Erfordernisse einer gesetzlichen Regelung kryptographischer Verfahren seit Mitte 1995 Fortschritte gemacht?

    Wenn ja, welche?

15. Beabsichtigt die Bundesregierung, bei den angekündigten gesetzlichen Regelungen einer elektronischen Unterschrift, die funktional einem Verschlüsselungssystem gleichkommt, die Systeme einer Lizensierung zu unterwerfen?

    Wenn ja, nach welchen Kriterien soll die Lizensierung geschehen, vor allem auch im Hinblick auf die Sicherheit der Systeme?

16. Welches Modell einer Schlüsselverwaltung strebt die Bundesregierung dabei an?

17. Beabsichtigt die Bundesregierung bei den genannten Systemen eine Beschränkung der Schlüssellänge?

18. Hält es die Bundesregierung für notwendig, die Nutzung von bestimmten Kryptosystemen einzuschränken bzw. zu verbieten?

19. Wie realistisch ist nach Ansicht der Bundesregierung die Annahme, eine Beschränkung von Kryptiersystemen auf einige zugelassene sichere die Abhörmöglichkeiten für Strafverfolgungsbehörden und Nachrichtendienste?

20. Wie passen nach Ansicht der Bundesregierung ihre Pläne einer Regelung der elektronischen Unterschrift zu den Plänen sowohl auf EU-Ebene als auch den unterschiedlichen Plänen zur Kryptographie auf der Ebene der OECD-Staaten, und sieht die Bundesregierung Probleme bei der Abstimmung?

21. Wie reagiert die Bundesregierung auf den Standpunkt der US-Administration, bei Export und Nutzung von asymmetrischen Kryptiersystemen auf solche Systeme hinzuwirken, die sicherstellen, daß Strafverfolgungsbehörden und Geheimdienste sowohl eingehende als auch ausgehende elektronische Kommunikation in bestimmten Fällen entschlüsseln können?

22. Welche Ministerien, Behörden und Ämter des Bundes sind zum gegenwärtigen Stand über das Internet erreichbar, in welcher Weise sind diese Systeme mit den übrigen DV-Systemen der jeweiligen Einrichtungen verbunden, und wie werden dabei die Sicherheit und Integrität dieser Systeme gewährleistet?

23. Zwischen welchen Behörden findet ein Datenaustausch statt, und wie wird dieser gesichert?

    In welchem Umfang hat das BSI Sicherheitskonzepte dafür erarbeitet?

24. Hat es bei einem derartigen Datenaustausch Sicherheitsanalysen durch den Bundesrechnungshof gegeben, und zu welcher Bewertung ist dieser gekommen?

25. Ist ein Ministerium, eine Behörde oder ein Amt im Verantwortungsbereich des Bundes jemals Opfer eines „Hackers" geworden?

    Wenn ja, um welche Behörde handelte es sich, wurde ein Angreifer identifiziert, ein Verfahren eingeleitet, und zu welchem Ergebnis kam dies?

    Wurden überdies Daten manipuliert oder zerstört?

26. Ist der Bundesregierung die amerikanische Software „PROMIS" (Prosecutor's Management System) bekannt, und ist sie in ihrem Verantwortungsbereich im Einsatz?

    Wenn ja, zu welchem Zweck und bei welcher Behörde?

27. Hat die Bundesregierung für die Beschaffung von Software Richtlinien, in denen IT-Sicherheitsaspekte berücksichtigt werden?

28. Gibt es Bereiche, in denen nur sicherheitsgeprüfte Software zum Einsatz kommt?

    Wenn ja, welche?

29. Ist der Bundesregierung in einer Einrichtung des Bundes jemals ein Softwareprodukt zur Kenntnis gelangt, das ein unerklärliches Sicherheitsloch – eine Sicherheits-trapdoor – auswies?

    Wenn ja, um welche Software handelte es sich?

30. Lassen sich derartige Sicherheitslöcher nach Erkenntnissen des BSI ohne Kenntnis des Quellcodes systematisch aufspüren?

    Wenn ja, mit welchem Aufwand?

31. Trifft es nach Kenntnis der Bundesregierung zu, daß bundesdeutsche „Hacker", die in den 80er Jahren in bestimmte Rechnersysteme in den USA eindrangen, ein Sicherheitsloch in den VAX/VMS-Betriebssystemen der Versionen 4.4 und 4.5 benutzten?

Bonn, den 2. Februar 1996

Dr. Manuel Kiper
Joseph Fischer (Frankfurt), Kerstin Müller (Köln) und Fraktion

Druck: Thenée Druck, 53113 Bonn, Telefon 91781-0
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon (02 28) 3 82 08 40, Telefax (02 28) 3 82 08 44
ISSN 0722-8333